

Data Processing Addendum

Vizbl Systems, Inc.

Effective Date: August 4, 2026

Last Updated: August 4, 2026

This Data Processing Addendum ("DPA") forms part of the agreement between Vizbl Systems, Inc., a Delaware corporation ("Vizbl"), and the customer identified in the applicable agreement or Order Form ("Customer") to the extent Vizbl Processes Customer Personal Data on behalf of Customer in connection with the Services.

Capitalized terms not defined in this DPA have the meanings given to them in the applicable agreement between Vizbl and Customer (the "Agreement"). This DPA applies only to Customer Personal Data Processed by Vizbl as a Processor, Service Provider, or Contractor on behalf of Customer. It does not apply to Personal Data for which Vizbl acts as an independent Controller or Business, including business contact, billing, account administration, security, fraud-prevention, and service-analytics data that Vizbl determines the purposes and means of Processing for, as described in Vizbl's Privacy Policy.

1. Definitions

"Applicable Data Protection Laws" means all laws and regulations applicable to the Processing of Customer Personal Data under the Agreement, including, where applicable, the EU General Data Protection Regulation 2016/679 ("EU GDPR"), the United Kingdom GDPR ("UK GDPR"), the Swiss Federal Act on Data Protection ("Swiss FADP"), the California Consumer Privacy Act as amended by the California Privacy Rights Act ("CCPA/CPRA"), and other applicable U.S. state privacy laws.

"Customer Personal Data" means Personal Data or Personal Information Processed by Vizbl on behalf of Customer in connection with the Services.

"Controller," "Processor," "Business," "Service Provider," "Contractor," "Consumer," "Data Subject," "Personal Data," "Personal Information," "Process," "Processing," "Sell," and "Share" have the meanings given under Applicable Data Protection Laws.

"Customer Content" means data, images, photographs, video, audio, text, prompts, product information, catalog information, 3D models, CAD files, digital assets, configuration data, and other content submitted to, stored in, generated through, or otherwise Processed by the Services for Customer.

"AI Inputs" means prompts, photographs, video frames, reference images, product images, body images, face images, hand images, room images, vehicle images, dimensions, metadata, and other information submitted to AI-enabled Services.

"AI Outputs" means generated, transformed, enhanced, segmented, rendered, classified, recommended, or otherwise machine-produced content or data created through AI-enabled Services.

"Security Incident" means a breach of security that results in the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Customer Personal Data Processed by Vizbl on behalf of Customer. Security Incident does not include unsuccessful attempts or activities that do not compromise Customer Personal Data, such as pings, port scans, denial-of-service attempts, unsuccessful login attempts, or similar events.

2. Roles and Scope

For Customer Personal Data, Customer is the Controller or Business and Vizbl is the Processor, Service Provider, or Contractor, unless otherwise stated in the Agreement or required by Applicable Data Protection Laws.

Customer determines the purposes and essential means of Processing and is responsible for the lawfulness of Customer's collection, use, disclosure, and instructions. Customer represents and warrants that it has provided all required notices and obtained all consents, authorizations, legal bases, permissions, and rights necessary for Vizbl to Process Customer Personal Data under the Agreement.

If Customer is itself a Processor acting for another Controller, Customer represents that its instructions to Vizbl are authorized by that Controller and that Customer is permitted to appoint Vizbl as a Subprocessor.

3. Processing Instructions

Vizbl will Process Customer Personal Data only: (a) to provide, secure, support, maintain, monitor, troubleshoot, and operate the Services; (b) on Customer's documented instructions, including the Agreement, Order Form, Statement of Work, service configuration, feature selections, support requests, and use of the Services; (c) as necessary to comply with applicable law; and (d) as otherwise permitted by this DPA and Applicable Data Protection Laws.

Where applicable law requires Vizbl to Process Customer Personal Data other than on Customer's documented instructions, Vizbl will inform Customer of that legal requirement before Processing, unless applicable law prohibits such notice.

Vizbl will promptly inform Customer if, in Vizbl's reasonable opinion, an instruction infringes Applicable Data Protection Laws. Vizbl may suspend the affected Processing until Customer modifies or confirms the instruction. Vizbl does not provide legal advice and is not responsible for determining whether Customer's business practices or instructions comply with law.

4. Vizbl Services and Product Coverage

The DPA applies to the Services identified in the applicable Agreement or Order Form. Depending on Customer's configuration, the Services may include the following current Vizbl product families and related capabilities:

- Core AR & 3D: Web AR Viewer, 3D Viewer, Standard AR, 3D+AR Viewer, One-Click AR, Multi-Item AR, Multi-AR, smart placement, product configurators, variants, materials, finishes, modular layouts, share links, snapshots, QR-code access, and analytics.
- AR Rugs: photo-based, true-scale rug, runner, and carpet visualization generated from catalog imagery and dimensions.
- AR Flooring: AI-assisted floor detection, segmentation, wall-to-wall replacement, plank or tile scaling, orientation, and texture visualization for hardwood, parquet, laminate, vinyl, tile, stone, carpet, and related finishes.
- AR Wall Art: wall detection, photo-based and camera-based wall placement, frame and size variants, gallery-wall layouts, split-canvas layouts, perspective correction, and AI-assisted surface detection.
- Vizbl Showroom AR: branded or configured iPad-based catalog and AR presentation for retail floors,

on-site consultations, outdoor structures, pools, spas, saunas, sheds, gazebos, pergolas, grills, fences, appliances, kiosks, vending machines, payment terminals, specialty equipment, and other large products.

- Construction AR: on-site visualization of flooring, paint, tile, fixtures, plumbing products, electrical devices, smart-home equipment, security systems, finishes, selections, proposals, and sign-off workflows.
- AutoFit AI: AI-assisted live or photo-based wheel and rim segmentation, replacement, size and finish comparison, and vehicle visualization.
- Vizbl Try-On / AI Photo Try-On: AI-assisted visualization of fashion, clothing, eyewear, jewelry, watches, rings, bracelets, earrings, hats, scarves, accessories, and other products on Customer-provided or End-User-provided photographs.
- AI Home Staging and AI Generation: AI-assisted placement, transformation, generation, or editing of products, rooms, scenes, imagery, marketing visuals, product previews, and related content.
- AR Public Catalog and Catalog AR: product publication, discovery, likes, ratings, reviews, saved boards, shares, product pages, AR launches, referral links, and related public-catalog functionality at Vizbl-hosted domains.
- Mobile and Distribution: WebAR, share links, QR codes, iOS App Clips, native iOS and Android SDKs, mobile applications, and other distribution surfaces.
- Developer and Integration Services: REST APIs, webhooks, SDKs, embed components, plugins, integrations, bulk uploads, SKU mapping, variants, analytics, and supported ecommerce platform connections.
- 3D Modeling and Digital Asset Services: creation, conversion, optimization, compression, texturing, rendering, format normalization, and delivery of 3D, CAD-derived, GLB, USDZ, FBX, OBJ, image, and related assets.
- Professional Services, pilots, proofs of concept, implementation, onboarding, training, hardware bundles, and custom enterprise solutions described in an Order Form or Statement of Work.

5. Categories of Data Subjects

Data Subjects may include Customer personnel, administrators, employees, contractors, Authorized Users, sales associates, designers, developers, support contacts, shoppers, website visitors, app users, public-catalog users, leads, business contacts, and other individuals whose Personal Data is submitted to or Processed through the Services.

6. Categories of Customer Personal Data

Depending on the selected Services, Customer Personal Data may include account and identity data; business contact data; user identifiers; authentication and access data; device, browser, operating-system, network, IP-address, log, telemetry, usage, event, and analytics data; support communications; lead-form and CRM-export data; product interaction and shopping activity; saved scenes, boards, ratings, reviews, and shares; uploaded images, photographs, videos, camera-derived inputs, and visual content; body, face, hand, ear, room, wall, floor, vehicle, and environment images; prompts and AI Inputs; AI Outputs; product, catalog, SKU, configuration, asset, dimension, and metadata

that identifies or can be linked to an individual; and other Personal Data submitted by Customer or its users.

Customer must not submit Social Security numbers, government identifiers, financial account credentials, payment-card data, precise health data, genetic data, biometric templates used for unique identification, children's data, or other highly sensitive data unless the applicable Order Form expressly authorizes that Processing and the parties agree on additional safeguards.

7. Nature, Purpose, and Duration

The nature of Processing may include collection, receipt, recording, organization, structuring, storage, hosting, retrieval, consultation, access, transmission, rendering, visualization, conversion, compression, segmentation, classification, generation, transformation, analysis, support, deletion, and other operations necessary to provide the Services.

The purposes are to provide, secure, support, maintain, troubleshoot, improve, and operate the Services selected by Customer; enable AR, 3D, AI, catalog, integration, analytics, collaboration, lead, and professional-service functionality; respond to support requests; prevent abuse and fraud; and comply with law.

Processing continues for the term of the Agreement and any limited post-termination period permitted by this DPA, the Agreement, or applicable law.

8. AI, Computer Vision, AR, and Image Processing

Certain Services use artificial intelligence, generative AI, machine learning, computer vision, segmentation, pose estimation, surface detection, object detection, image transformation, image generation, model generation, recommendation, classification, rendering, or similar automated techniques.

Customer is responsible for determining whether use of AI-enabled Services is lawful and appropriate for its use case, for providing required notices and choices, and for obtaining valid consent where images, camera inputs, body images, face images, hand images, room images, vehicle images, or other Personal Data are submitted.

Vizbl will not use Customer Personal Data to train a general-purpose or shared AI model for the benefit of other customers or third parties unless Customer expressly authorizes such use in writing. Vizbl may use aggregated or de-identified data that does not identify Customer or any individual and is not reasonably capable of re-identification for security, analytics, benchmarking, quality assurance, and improvement of the Services.

Customer acknowledges that third-party AI providers may Process AI Inputs and AI Outputs as Subprocessors where identified on Vizbl's Subprocessor list or otherwise disclosed in accordance with this DPA.

9. Customer Content, Camera Data, and End-User Inputs

Customer is responsible for the content and legality of Customer Content and for ensuring that Customer has authority to upload, photograph, scan, record, analyze, generate, publish, and otherwise Process it

through the Services.

Where a feature performs processing locally on an End User's device, data that remains solely on the device and is not transmitted to Vizbl is not Customer Personal Data Processed by Vizbl. Customer must not rely on a statement that camera frames remain local unless the applicable product documentation expressly confirms that behavior for the specific feature and version used.

Customer will configure the Services to minimize collection of Personal Data and will not use the Services for covert surveillance, facial recognition for unique identification, employment decisions, credit decisions, healthcare diagnosis, law-enforcement identification, or other high-risk purposes unless expressly authorized in writing by Vizbl and permitted by law.

10. Confidentiality

Vizbl will ensure that personnel authorized to Process Customer Personal Data are subject to confidentiality obligations and receive appropriate privacy and security instructions. Access will be limited to personnel who require it for the Services, support, security, compliance, or other permitted purposes.

11. Security Measures

Vizbl will implement and maintain commercially reasonable administrative, technical, and organizational measures designed to protect Customer Personal Data against accidental or unlawful destruction, loss, alteration, unauthorized disclosure, or access. The measures are described in Schedule 2 and may evolve to reflect changes in technology, risk, and the Services, provided that Vizbl will not materially reduce the overall level of protection during the term.

No system is completely secure. Vizbl does not warrant that Security Incidents will never occur. Customer is responsible for securely configuring and using the Services, managing Authorized Users, protecting credentials, maintaining its own systems and backups, and promptly notifying Vizbl of suspected compromise.

12. Subprocessors

Customer provides general written authorization for Vizbl to engage affiliates and third-party Subprocessors to Process Customer Personal Data. Vizbl will maintain a current list of Subprocessors through a website, portal, or upon request.

Where required by Applicable Data Protection Laws, Vizbl will provide at least fifteen (15) days' prior notice of a new Subprocessor that will materially Process Customer Personal Data, except where immediate engagement is reasonably necessary for security, service continuity, legal compliance, or to avoid material disruption. Customer may object during the notice period on reasonable and documented data-protection grounds. The parties will work in good faith to address the objection. If no commercially reasonable alternative is available, Vizbl may terminate the affected Service and refund prepaid recurring fees for the unused terminated period as Customer's sole remedy.

Vizbl will impose data-protection obligations on Subprocessors that are no less protective in material respects than the obligations applicable to Vizbl under this DPA. Vizbl remains responsible for each Subprocessor's performance to the extent required by Applicable Data Protection Laws.

13. International Transfers

Customer acknowledges that Customer Personal Data may be Processed in the United States and other jurisdictions where Vizbl or its Subprocessors operate.

Where a legally recognized transfer mechanism is required, the parties will rely on an applicable adequacy decision, the EU Standard Contractual Clauses, the UK International Data Transfer Addendum or International Data Transfer Agreement, the Swiss adaptations, or another lawful mechanism. Schedule 3 describes the intended transfer framework. The official text of any mandatory transfer clauses will control and will not be modified except as permitted by the issuing authority.

14. Data Subject Requests

Taking into account the nature of Processing, Vizbl will provide reasonable assistance through appropriate technical and organizational measures to help Customer respond to requests to access, correct, delete, restrict, port, or object to Processing of Customer Personal Data, to the extent required by Applicable Data Protection Laws.

Customer is responsible for receiving, authenticating, and responding to requests. If Vizbl receives a request relating to Customer Personal Data, Vizbl may direct the requester to Customer unless prohibited by law. Vizbl may charge reasonable fees for assistance that is excessive, repetitive, or outside standard functionality, to the extent permitted by law.

15. Security Incident Notification

Vizbl will notify Customer without undue delay after becoming aware of a Security Incident involving Customer Personal Data. Notice may be delivered to Customer's designated security, privacy, legal, or administrative contact.

To the extent information is reasonably available, Vizbl will describe the nature of the Security Incident, the categories of affected Data Subjects and data, likely consequences, and measures taken or proposed to contain, investigate, and remediate it. Vizbl may provide information in phases as the investigation progresses.

Customer is responsible for determining whether to notify regulators, Data Subjects, customers, or other parties and for the content and timing of those notices. Vizbl's notice or response is not an admission of fault, wrongdoing, or liability.

16. Assistance with Compliance

Taking into account the nature of Processing and information available to Vizbl, Vizbl will provide reasonable assistance with Customer's obligations concerning security, breach notifications, data-protection impact assessments, and prior consultation, to the extent required by Applicable Data Protection Laws.

Customer will provide sufficient information and will reimburse Vizbl for reasonable costs of assistance that is extraordinary, customized, or not included in the Services, except where the need for assistance results from Vizbl's breach of this DPA.

17. Return and Deletion

At Customer's written election and subject to the Agreement, Vizbl will delete or return Customer Personal Data after termination of the affected Services and delete remaining copies, except to the extent retention is required by applicable law.

Customer Personal Data in routine backups may remain until overwritten or deleted in the ordinary course, provided it remains protected under this DPA, is not restored or otherwise Processed except for disaster recovery, security, or legal purposes, and is deleted according to Vizbl's standard backup cycles.

Vizbl may retain de-identified data that cannot reasonably identify Customer or any individual. Customer is responsible for exporting Customer Personal Data before termination where export functionality is available.

18. Audits and Information Rights

Vizbl will make available information reasonably necessary to demonstrate compliance with this DPA, which may include security summaries, policies, questionnaires, certifications, or independent audit reports that Vizbl actually maintains.

After reviewing available documentation, Customer may conduct an audit where reasonably necessary to demonstrate compliance with Article 28 GDPR or comparable Applicable Data Protection Laws. Audits are limited to once in any twelve-month period unless required by a supervisory authority or following a Security Incident materially affecting Customer Personal Data; require at least thirty (30) days' prior written notice; occur during normal business hours; must not unreasonably interfere with operations; and are at Customer's expense.

Auditors must be independent, qualified, not competitors of Vizbl, and bound by confidentiality. Audits may not access data of other customers, source code, penetration-test materials, vulnerability details, trade secrets, or information that would compromise security. Vizbl may satisfy an audit request through recent third-party reports or remote review where reasonably sufficient.

19. CCPA/CPRA and U.S. State Privacy Terms

To the extent Customer Personal Data is Personal Information subject to the CCPA/CPRA, Customer discloses it to Vizbl only for the limited and specified business purposes described in the Agreement, this DPA, and Customer's documented instructions. Vizbl will act as a Service Provider or Contractor and will not Sell or Share such Personal Information except as permitted by the CCPA/CPRA.

Vizbl will not retain, use, or disclose such Personal Information outside the direct business relationship with Customer or for a commercial purpose other than the specified purposes, except as permitted by law. Vizbl will provide the same level of privacy protection required of Customer under the CCPA/CPRA with respect to such Personal Information.

Vizbl will notify Customer if Vizbl determines it can no longer meet its applicable obligations. Upon reasonable notice and subject to the security and audit limits of this DPA, Customer may take reasonable and appropriate steps to help ensure compliant use and to stop and remediate unauthorized use.

Vizbl certifies that it understands and will comply with the restrictions in this Section.

20. EU GDPR, UK GDPR, and Swiss Processor Terms

To the extent the EU GDPR, UK GDPR, or Swiss FADP applies, Vizbl will comply with the processor obligations applicable to Vizbl, including Processing on documented instructions; confidentiality; appropriate security; Subprocessor controls; assistance with Data Subject rights and compliance obligations; deletion or return; and audit and information rights.

Customer grants general written authorization for Subprocessors subject to Section 12. If mandatory standard clauses apply, those clauses prevail over conflicting provisions of this DPA to the extent of the conflict.

21. Customer Responsibilities

- Comply with Applicable Data Protection Laws and the Agreement.
- Provide required notices and obtain required consents, permissions, and legal bases.
- Ensure Customer Personal Data, Customer Content, AI Inputs, and instructions are lawful, accurate, appropriate, and limited to what is necessary.
- Configure and use the Services consistently with Customer's obligations, including age restrictions, consent choices, retention settings, and access controls.
- Respond to Data Subject requests and regulatory inquiries.
- Maintain backups and security for Customer systems, credentials, devices, networks, integrations, and exports.
- Not submit prohibited or highly sensitive data unless expressly authorized in writing.
- Independently review and approve AI Outputs, visualizations, measurements, generated content, and automated results before relying on or publishing them.

22. Independent Controller Processing

Vizbl may Process limited Personal Data as an independent Controller or Business for legitimate business operations such as account creation, billing, customer relationship management, service administration, security, fraud prevention, abuse detection, legal compliance, product analytics, and communications. Such Processing is governed by Vizbl's Privacy Policy and not by this DPA, except where Applicable Data Protection Laws require otherwise.

Vizbl will not combine Customer Personal Data received in its Service Provider or Processor role with Personal Data received from another person or collected from Vizbl's own interaction with a Consumer except as permitted by Applicable Data Protection Laws.

23. De-identified and Aggregated Data

Vizbl may create and use aggregated or de-identified data derived from the Services for security, fraud prevention, analytics, benchmarking, service operation, and improvement, provided that the data does not identify Customer or any individual and is not reasonably capable of being associated with or linked to them. Vizbl will maintain reasonable measures designed to prevent re-identification and will not attempt to re-identify such data except to test the effectiveness of de-identification as permitted by law.

24. Liability

Each party's liability arising out of or relating to this DPA is subject to the exclusions, limitations, disclaimers, and aggregate liability cap in the Agreement, unless Applicable Data Protection Laws prohibit their application. This DPA does not create a separate, additional, or cumulative liability cap.

To the maximum extent permitted by law, Vizbl is not responsible for claims, penalties, damages, or costs caused by Customer's unlawful collection, notices, consents, instructions, configuration, content, use of AI Inputs or AI Outputs, use of the Services for prohibited purposes, or failure to comply with Customer's obligations.

25. Conflict and Order of Precedence

If this DPA conflicts with the Agreement, this DPA controls solely with respect to Processing of Customer Personal Data. The Agreement controls in all other respects. If mandatory Standard Contractual Clauses or another mandatory transfer mechanism conflicts with this DPA, the mandatory clauses control for the applicable transfer.

26. Updates

Vizbl may update this DPA from time to time. An update will not materially reduce the overall protection of Customer Personal Data during the then-current subscription term, except where reasonably necessary to comply with law, address a security or privacy risk, reflect changes in mandatory transfer mechanisms, or maintain compatibility with the Services or Subprocessors. Materially adverse changes otherwise apply no earlier than Customer's next renewal term.

27. Notices and Contact

Privacy and DPA notices to Vizbl must be sent to privacy@vizbl.com or legal@vizbl.com, with a copy to any address specified in the Agreement. Customer is responsible for keeping its privacy, security, legal, and administrative contacts current.

Schedule 1 - Details of Processing

Item	Details
Subject matter	Processing of Customer Personal Data to provide the Services identified in the Agreement, Order Form, or Statement of Work.
Duration	The term of the applicable Services plus the limited retention periods permitted by the DPA or law.
Nature of Processing	Collection, receipt, storage, hosting, access, transmission, rendering, visualization, conversion, compression, segmentation, classification, generation, transformation, analysis, retrieval, support, and deletion.
Purposes	Providing, securing, supporting, maintaining, troubleshooting, improving, and operating the selected Vizbl Services.

Data Subjects	Customer personnel, Authorized Users, contractors, sales associates, shoppers, website visitors, app users, public-catalog users, leads, business contacts, and other individuals whose data is submitted by or for Customer.
Personal Data	Account, contact, authentication, device, network, logs, usage, analytics, support data, lead data, uploaded images and media, camera-derived inputs, prompts, AI Inputs, AI Outputs, saved scenes, product interaction data, reviews, ratings, and other data described in Section 6.
Sensitive Data	Not permitted unless expressly authorized in an Order Form or written amendment with additional safeguards.
Frequency	Continuous, periodic, or initiated by Customer, Authorized Users, End Users, APIs, SDKs, integrations, or automated workflows.
Retention	For the Service term and then according to Section 17, Customer configuration, the Agreement, and applicable law.

Schedule 2 - Technical and Organizational Measures

Item	Details
Governance and risk management	Privacy and security policies; defined responsibilities; risk-based controls; periodic review.
Access control	Role-based access; least privilege; authentication controls; administrative access restrictions; access review.
Credential security	Password controls and multi-factor authentication for privileged access where supported and appropriate.
Encryption	TLS or comparable encryption in transit; encryption at rest where supported and appropriate for the relevant storage system.
Logging and monitoring	Security logging, system monitoring, alerting, and investigation procedures appropriate to the Services.
Secure development	Change management, code review, dependency management, testing, and remediation practices appropriate to the Services.
Vulnerability management	Vulnerability identification, prioritization, patching, and remediation processes based on risk.
Incident response	Documented procedures for identification, containment, investigation, remediation, recovery, and notification.
Availability and resilience	Backups, redundancy, recovery procedures, and business-continuity measures appropriate to the Services; no separate service level is created by this Schedule.
Personnel	Confidentiality obligations, access limitations, and privacy/security awareness for personnel with access.
Vendor management	Risk-based review and contractual controls for Subprocessors.
Data minimization and deletion	Controls designed to limit Processing to relevant data and delete or de-identify data according to applicable retention practices.

Physical security	Physical and environmental safeguards provided by Vizbl or its hosting and infrastructure providers.
AI and image safeguards	Access controls, provider restrictions, prompt/input handling controls, moderation or safety features where applicable, and restrictions on general-model training as stated in Section 8.

Schedule 3 - International Data Transfer Framework

Item	Details
EU transfers	Where required, the 2021 EU Standard Contractual Clauses apply using Module 2 (Controller to Processor) or Module 3 (Processor to Processor), as appropriate. The parties must complete and execute the required annexes or an applicable transfer addendum.
UK transfers	Where required, the UK International Data Transfer Addendum to the EU SCCs or the UK International Data Transfer Agreement applies, as selected in the Agreement or transfer addendum.
Swiss transfers	Where required, the EU SCCs apply with adaptations necessary under the Swiss FADP, including references to the competent Swiss authority and Swiss law where applicable.
Priority	The official mandatory clauses control over conflicting provisions for the relevant transfer. Their text may not be modified except as permitted by the issuing authority.
Transfer assessments	Each party will provide information reasonably necessary for an applicable transfer impact assessment, subject to confidentiality, security, legal, and proportionality limitations.
Supplementary measures	Vizbl may use technical, contractual, and organizational supplementary measures appropriate to the transfer and the Services.